User Guide | September 2021

Vorex and Authanvil - SAML 2.0 Single Sign-On (SSO) Just-in-Time (JIT) Provisioning

Release 5.4.0 | Version 1.0



www.kaseya.com

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement.

Contents

AuthAnvil Setup	4
Download the Certificate	
Vorex Setup	12
AuthAnvil Application Assignment	13
Enable Two Way SAML Login	15
Enable JIT Provisioning	17

AuthAnvil Setup

Assuming you have an active AuthAnvil (https://subdomain.authanvil.com/) account.

Kaseya Kaseya		K
	@AuthAnvil [∞]	
	Password Forgot Password Log in	
	© Copyright Kaseya Limited Help & Support v1.0.42.1	

In order to setup Vorex with AuthAnvil you need to have a user group that can associate with the Vorex SSO configuration.

Creating a new group.

1 Log in to AuthAnvil and navigate to Directory Manager > Groups.



3 Give a name to your group.

2

4 Click the Add Group button.

Now a new group is created.

Setting up Vorex with AuthAnvil.

1 Navigate to SSO Manager.



💮 AuthAnvil"				٩	🔒 data kanaharana 🔣
SSO Manager > Application	on Library			docsteam	· <u>÷</u> :
Launchpad	Application Name -	Users	Authentication Policy	Last Launched	
Password Vaults	U Service Now	0	Default Auth Policy	Never	:
Getting Started					
Directory Manager					
Password Server					
III Just In Time 2FA					
Auth Manager					
Policy Manager					
🗗 SSO Manager 🔶 1					
Application Library					
Workflow Requests					
License Manager					
					2
Help & Support					+

Click the button then search for Vorex and then select Vorex from the list.

AuthAnvil [~]					e daria kovshar	ova 🔣
SSO Manager >	Application Library			docsteam		÷ :
Launchpad	Add new Application to the Library					
Password Vaults	Find an app in the catalog Q BMS	Workflow Category -				:
Getting Started	Custom Application	Create a custom application	Federated (SP-Init), Federated (IdP-Init)			
Directory Manage	📯 Kaseya BMS <	A next-generation business management solution.	Federated (SP-Init)			
Password Server						
III Just In Time 2FA						
Auth Manager						
Policy Manager						
I↑ SSO Manager						
Application L						
Workflow Rev						
E License Manager						0
			Cance	Add Application		0
Help & Support						+

- 4 In the Add new Application to the Library window, select the Application is Enabled checkbox.
- 5 Click the **Add Application** button at the bottom right of the screen.

3



Now the application added.

6 Navigate to Permissions tab.

🔮 AuthAnvil"	🖗 AuthAnvil					
SSO Manager > Kaseya I	BMS				docsteam -	
Launchpad	Application Configuration	Protocol Setu	up Attribute Transformation	6 Permissi	ons Signing and Encryption	
Password Vaults				U U	Inderstanding Application Configuration	
🖈 Getting Started	\sim	1		A a c	AuthAnvil supports federation to applications. Each application has a unique configuration. Some configuration elements are required while others are	
Directory Manager	Change In	nage		a	optional.	
Password Server	Application is Enabled				 Enabling Applications: Applications can be enabled or disabled without having to be deleted Display Name: An identifier a user will see in the 	
Just In Time 2FA	Give your application a name				Portal Application Image: An icon that is used to identify	
Auth Manager	Address and a second and a seco				 Preferred image size is 64 x 64 pixels Image should be smaller than 100 x 100 pixels 	
Policy Manager	Default Auth Policy	•			 Image must be smaller than 100kb Supported formats are: PNG, GIF, JPEG/JPG 	
SSO Manager						
Application Library						
Workflow Requests						
License Manager						
Help & Support					Save Changes	

- 7 Click the Add Group button and select the group you created.
- 8 Click the Add Groups button to finish setup.



9 Navigate to Attribute Transformation tab.

٢	AuthAnvil						🌲 😝 daria kovsharova 🔣
S	60 Manager > Kaseya Bl	MS					docsteam -
	Launchpad	Application Configuration	Protocol Setup	Attribute Transformation		Permissions	Signing and Encryption
C	Password Vaults	Group Access	9			Application Permissions	
¢	Getting Started	() Changes to group membership will n	ot affect users until they sign out and sign	n back in again.		Applications support grou You can specify which grou	up-based permissions for users. Dups can access this application
	Directory Manager	Group Name	Last Modified			launch this application.	or a descendent group can
Ô	Password Server	PSA User	10/25/2019		:		
	Just In Time 2FA	Domeuro Selected			Add Crowno		
÷.	Auth Manager	Remove Selected			Add Gloups		
0	Policy Manager						
(†)	SSO Manager						
	Application Library						
	Workflow Requests						
⊟	License Manager						
0	Help & Support						Save Changes

10 Change the CompanyName attribute

1	AuthAnvil						🛕 🙁 daria kovsharova 🔀
SS	0 Manager > Kaseya BN	MS					docsteam -
	Launchpad	Application Configuration	Protocol Setup	Attribute Transformation	Pe	rmissions	Signing and Encryption
C	Password Vaults	 Just issue an attribute as the usernal 	ne			Attribute Transformation	on
¢	Getting Started	 Specify custom attribute transform 				AuthAnvil supports attr This allows you to map claims of any type.	ibute issuance transformation. any attribute(s) of a user to
	Directory Manager	Attribute Value		Send As		Just Issue Attribu	ite as Username: Allows you to
0	Password Server	{User.PrincipalName}	-> http://schemas.xmlsoap.	org/ws/2005/05/identity/claims/nameidentifier	Remove	 use a predetined token profile and just attribute should be used for the usern. Specify Custom Attribute Transform: specify custom mappings for multiple 	e used for the username. ttribute Transform: Allows you to appings for multiple attributes.
Ð	Just In Time 2FA Auth Manager	{User.EmailAddress}	=>	email	Remove	Attributes can be acces notation {User.EmailAddr	used on an object using dot ess}. They can be used inline with
٢	Policy Manager	CompanyName	⇒ Set you	CompanyName	Remove	other text {User.PrincipalName}@example.com attributes can be used in a single statem {User.Id}@{User.Domain} .	in a single statement
(†)	SSO Manager	{User.PrincipalName}@{User.Domain}	company here	username	Remove	Extended Properties	
	Application Library	{User.Groups}	ε>	securitygroup	Remove	 Format: Specify v follows. Display Name: A Attribute Name Q 	hat format the claim value friendly name for the claim. ualifier: The security or
	License Manager	Add Custom Attribute Map				administrative do This attribute pro- identifiers from di collision. • SP Name Qualifie with the name of providers. This at	main that qualifies the identifier. vides a means to federate sparate user stores without rr: Further qualifies an identifier a service provider or affiliation of tribute provides an additional
0	Help & Support						Save Changes

Protocol Setup

- 1 Navigate to the **Protocol Setup** tab.
- 2 For Assertion Consumer URL, change the base url to the base url of your BMS server. In the example below, the base url is nalbmspreview.kaseya.com.
- 3 For Service Entity ID, change the base url to the base url of your BMS server. In the example below, the base url is nalbmspreview.kaseya.com.
- 4 Save your changes.

Application Configuration	Protocol Setup	Attribute Transformation
Protocol Type		
SAML SP-Init		
Assertion Consumer Service URL		
https://	-	—
Allow Multiple Audiences		Your URL
Service Entity ID (Issuer)		
https://		
Identity Issuer		
https://		
Token Lifetime (Minutes)		
60		
Advanced Cettings		
Advanced Settings		
Configure advanced settings for this application		
View Federation Metadata		

Download the Certificate

- 1 Navigate to AuthAnvil > SSO Manager.
- 2 Open the Vorex application.

٢	AuthAnvil					≜ ⊖	daria kovsharova 🛛 Ҟ
SS	60 Manager > Applicatio	on Libr	ary			docsteam	• = :
	Launchpad		Application Name 🔺	Users	Authentication Policy	Last Launched	
C	Password Vaults	\sim	PulsewayPSA	0	Default Auth Policy	Never	:
¢	Getting Started	ወ	Service Now	0	Default Auth Policy	Never	:
	Directory Manager						
ø	Password Server						
	Just In Time 2FA						
Ð	Auth Manager						
٢	Policy Manager						
(†)	SSO Manager						
	Application Library						
	Workflow Requests						
	License Manager						
0	Help & Support						

3 Navigate to Signing and Encryption tab.

@ AuthAnvil~					🌲 😝 daria kovsharova 🔣
SSO Manager > Pulseway	yPSA				docsteam -
Launchpad	Application Configuration	Protocol Setup	Attribute Transformation	Permissions	Signing and Encryption
 Password Vaults Getting Started Directory Manager Password Server Just In Time 2FA Auth Manager Policy Manager SSO Manager Application Library Workflow Requests 	Change Image Change Image Change Change Image Change Image Change Change Change Image Change Change Change Image Change Image Change Change Change Change Change Change Change Chan			Understanding AuthAnvii supy application has configuration e optional. • Enabling or disabi • Display h • Display h • Applicati the appli • Pre • Imm • Imm • Sup	Application Configuration borts federation to applications. Each a unique configuration. Some lements are required while others are Applications: Applications can be enabled ed without having to be deleted lame: An identifier a user will see in the on Image: An icon that is used to identify ation in the Portal ferred image size is 64 x 64 pixels uge should be smaller than 100kb sported formats are: PNG, GIF, JPEG/JPG
License Manager					
Help & Support					Save Changes

4 Click the **Download** button.

💮 AuthAnvil [~]					🌲 😫 daria kovsharova 🔣
SSO Manager >					docsteam 👻
Launchpad	Application Configuration	Protocol Setup	Attribute Transformation	Permissions	Signing and Encryption
Password Vaults	Signing Certificate			Signing and Encry	yption
🖈 Getting Started	Subject CN=docsteam Signing	Certificate		AuthAnvil enables data sent to the a	s federation by signing and encrypting pplication.
Directory Manager	Issuer CN=docsteam Signing Valid Between 6/28/2019 - 6/26/2024	Certificate 1		Signing Cer the applicat	tificate: Used to sign the token issued to ion with a private key.
Password Server	Thumbprint 5328D8A6A6BD454E4	8D92CBCA33DDB73DAC0D34C		• Copy of the • Downl	certificate for easy copying. oad Certificate: Download a DER-
III Just In Time 2FA	<> Copy 👱 Download	←4	ϕ Generate new Cert	tificate encod • Generation a new	ed version of the certificate. ate new Certificate: Generate or upload Signing key. Warning: You will not be
Auth Manager				able to config	o sign into the application until it is ured with the new certificate.
Policy Manager				token again: • Copy (st an application public key. Certificate: Show CER-encoded version
SSO Manager				of the • Downl encod	certificate for easy copying. oad Certificate: Download a DER- ed version of the certificate.
Application Library				 Upload encryp to sign 	d new Certificate: Upload a new otion key. Warning: You will not be able
Workflow Requests				config	ured with the new certificate.
License Manager					
Help & Support					Save Changes

Vorex Setup

In Vorex we need to setup the system to enable SAML authentication and that can be achieved under Admin > My Company > Authentication.

In the "Single Sign On" tab, upload the certificate downloaded previously, and set "Enable Single Sign On via SAML" to **Yes**, then click Save.

Home / Authentication / Authentication Save (S) C Refresh (R) See Logs		
Single Sign On Authenticator		
Enable Single Sign On via SAML:	⊳	
SAML Login Endpoint URL:		
Certificate Information		
No Certificate detected.		
Upload Certificate Delete Certificate		
Auto-Provision Users:		

This will enable Vorex SAML authentication.

AuthAnvil Application Assignment

Once the application created, navigate to Directory Manager > Users then choose any user and add the assigned group for this user.

III Launchoad	Alternate Principal Names	kevin@getmytools.lo
+		User supports Just In Time 2FA
12 Getting Started	2FA Push	No authenticator has been registered
Directory Manager	One-Time Passcode	No token has been registered
± Users	Universal Second Factor (U2F)	No token has been registered
At Groups		6
Zz. Roles	- Memberships	
BII Organizations		
Y* Directory Sync	Roles	User (brist) Add Roles
BII Just in Time 2FA	Groups	No active groups for this user
Auth Manager		Add Groups
Policy Manager		
SSO Manager	 Trusted Devices 	2
License Manager		
		There aren't any trusted devices yet.

Now when the user assigned, go to Launchpad in the left menu then click on the Vorex SSO application you created to be redirected and logged in to Vorex.

1	AuthAnvil ⁻	
Му	Apps > All Apps	
	Launchpad	
Ŕ	Getting Started	2
	Directory Manager 1	PulsewayPSA
	Just In Time 2FA	
÷	Auth Manager	
٢	Policy Manager	
(†)	SSO Manager	
⊟	License Manager	

Enable Two Way SAML Login

In order to launch AuthAnvil during the Log in from Vorex. You need to enable two-way SAML integration. In order to do this, you will need your AuthAnvil Login URL that can be found here:

<u>ن</u>	AuthAnvil			
My	Apps > All Apps			
	Launchpad			
\$	Getting Started	~	Open link in new tab	
8	Directory Manager	Pulse	Open link in new window Open link in incognito window	
	Just In Time 2FA		Save link as	
Ð	Auth Manager	1	Copy link address Get image descriptions from Google	
۲	Policy Manager		Inspect	Ctrl+Shift+I
(†)	SSO Manager			
	License Manager			

Once you have this URL, you will need to save it in Vorex under the Authentication Page:

Admin Dechlorerd	Home / Authentication / Authentication					
 MyCompany v 	V See (D) C Reference (D) See Lags					
+ Locations	Single Sign On Authenticator					
Company Settings Outbound Email	MUS Fector Authentication (MFA) For those users who are not configured to use 550 percebelous you can enforce loff-for all users which will require the user to use an authenticator applicator such as Google Authenticator.					
Custom Fields Little	Require WAI for room500 users:					
Company News	Next Segade Allow were to advertise using your 300 application. One 300 is involved, you can configure each user to use 300 or not, via the tolenesk Authentication Type property on the user record train 300 advectories must applicate Set Set. 1.2					
 Administrative Work 	Enable Single Sign-On via SAMC:					
Automization	Sngli Inte					
Cyracon Insgration	SARL Logn English (III) Mga/					
Business Process C	Minimum automatical and a set and an and a set					
• HR	Certificate Name Centre Certificate Centre Date: 10/16/111					
• OM (Certificate Version 7 Certificate Darjes (2014) Certificate Darjes (2014) Certificate Darjes (2014) Certificate Darjes (2014) Certificate Strait Number (2014) Certificate Strait Strait Number (2014)					
Security 4	And Andee Machinetic ANEMI And Andee Machinetic ANEMI And Andee Machinetic ANEMI Andee Machinetic ANEMI Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMICANS Andee Machinetic ANEMIC AND Statements Andee Machinetic ANEMICANS Andee Machinetic ANEMIC AND AND Statements Andee Machinetic ANEMICANS Andee Machinetic ANEMIC AND AND AND					
B france C	Upload Certificate Deleta Certificate					

This will allow you to leverage the AuthAnvil Log in screen when users are trying to log in to Vorex. You can enable this on the User Level by updating the Authentication Type on the Employee Level:

sonal Details Contact	: Info Wages	Shifts	Associated Ac	counts	Associated Queues
User Name:*				Emp	p ID:*
EMploye				45	596
First Name:*				Mid	ldle Name:
First					
Last Name:				Em	ail Address:*
				er	mail
Job Title:*				Dep	partment:*
Administrator				•	Administration
Location:*				Em	ployment Type:*
Main Branch				·	Full Time
Manager:*				Hire	e Date:
Belle				·	
Termination Date:				Birt	h Date:
SSN:			0	Mar	rital Status:
Status:	Exter	nal:		Ger	nder:
Active InActive	•	'es 🔵 No			
External Authentication Ty	/pe:			Not	es:

Enable JIT Provisioning

IMPORTANT!	An a	additional attribute, DisplayN	ame	needs to be added in Passly for JIT provisioning.		
		 Just issue an attribute as the usern Specify custom attribute transform 	ame			
		Attribute Value		Send As		
		{User.PrincipalName}	=>	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	Remo	ve
		{User.EmailAddress}	=>	email	Remo	ve
		{User.Groups}	=>	securitygroup	Remo	ve
		{User.DisplayName}	=>	DisplayName	Remo	ve
		{User.PrincipalName}@{User.Domain}	=>	username	Remo	ve
		zahraa and co	=>	CompanyName	Remo	ve
		Add Custom Attribute Map				

In order to enable Just-in-Time (JIT) provisioning, you will need to do it from the Vorex Authentication page.

Admin Dechlored	application must support SAM, 2.0.		or the one include the record of the prop	e gior sie daer record. Toor abo	
O MyCompany -					
+ Locations	Enable Single Sign-On via SAML				
+ Company Settings	Single sign on UBL				
> Outpared Erect	https:/				
	SAML Legin Endpoint URL:				
 Custon Fields 	NEDEN				
> Las	Certificate Information				
 Company News 	Partificate Name Service Conferen	Certificate Created Date: 1011			
> Molidays	Certificate Version: J Certificate Senature Algorithm: shu356554	Certificate Expiry: 10/14/2004 Certificate Serial Number: 640	NY 15890555874342483080000035308		
> Administrative Work					
> Authentication	Upload Certificate Delete Certificate				
> If Oue Settings					
> Cytracom Integration	Auto-Previsioning for 350 To further leverage SAM, SSO, you may configure your SSO and/ or Client Access Surgesters in specific Client Accounts	application to auto-provision users on a just-in-time basis. When	n users are auto-provisioned, mapping rules	specify the creation of Employee users	
Business Process K					
	Auto-Provision Users:				
· ·	• 📼 🖂	4	r		
🗑 СМ — 🤄	Employee Defaults				
Security 4	Department	Location*		Security Roles*	
	Client Services	 Main Branch 	•	External Manager	•
00 Fearce 4	Employee Roles*	Manager*		Employment Type*	
🖌 Service Deak 💦 K	At tens checked	 global admin 	•	Contractor	•
-	job Tie*				
Inventory 4	An				

By default, all Users will take the Default Security Roles specified in the above Employee Defaults Section. In order to start mapping Active Directory Groups to Vorex Security Roles you will need to Add Mapping Rules as following:

Mapping Rules				
O Add O Delete				
ACTIONS DOBAN	SECURITY GROUP	ACCOUNT	MOUNTY NOLE	SECURITY NOLE
ii a	PSA Users		Employee	Project Manager

By adding multiple Rules, you can now start routing Active Directory Users to Vorex Security Roles based on Domain and Security Group.

Provision Users:						
		Add/Edit	×			
nployee Defaults				-		
epartment*		✓ Add/Edit Mapping Rule		surity Roles*		
Client Services	Þ	Domain		External Manager		
mployee Roles*				ployment Type*		
All items checked		Security Group*		Contractor		
b Tile*		PSA Users				
Administrator		Map user to				
		· Impleyer 0				
language Dr. Jan		Contact with Client Partial Access				
1994 E 1995		Onder .				_
		croer				
• • • • • • • • • • • • • • • • • • •		fan eile Beler				
Actions DOMAIN		Project Manager			NECURITY ROLE	
9.7		r opera manager			Project Managar	
					codece manades	
			Save Cancel			